METHOD, NODE AND COMPUTER READABLE MEDIUM FOR IDENTIFYING DATA IN A NETWORK EXPLOIT

ABSTRACT OF THE INVENTION

A method of identifying data comprised in a network exploit comprising receiving a packet by an intrusion prevention system maintained by a node of a network, the intrusion prevention system bound to a media access control driver and a protocol driver, invoking a signature analysis algorithm by the intrusion prevention system, and comparing the packet by the intrusion prevention system with a first rule set comprising a rule logically defining a packet signature is provided. A node of a network maintaining an instance of an intrusion prevention system, the node comprising a central processing unit, a memory module for storing data in machine-readable format for retrieval and execution by the central processing unit, and an operating system comprising a network stack comprising a protocol driver, a media access control driver and an instance of the intrusion prevention system bound to the protocol driver and the media access control driver, the intrusion prevention system comprising an associative process engine and an input/output control layer, the input/output control layer operable to receive a signature file generated from a network exploit rule comprising an operand, an operator and a mask, the input/output control layer operable to pass the signature file to the associative process engine, the associative process engine operable to analyze a data packet with the signature file and assign a logical value to the signature file dependent upon a result from the analysis is provided. A computer-readable medium having stored thereon a set of instructions to be executed, the set of instructions, when executed by a processor, cause the processor to perform a computer method of reading a data packet, selecting a set of a plurality of signature files from a plurality of sets of signature files, each respective signature file of the plurality of sets of signature files generated from a respective rule of at least one rule set comprised of a plurality of rules, and comparing the data packet with at least one signature file of the selected set is provided.

is provided.